UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

LEO THORBECKE and MARJORITA DEAN, individually and on behalf of all others similarly situated, Plaintiff, v. MCG HEALTH, LLC, a Washington limited liability company, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Leo Thorbecke and Marjorita Dean ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action against Defendant MCG Health, LLC ("MCG Health" or "Defendant") and allege as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

U.S.C. § 1367 because they form part of the same case or controversy as the claims within the Court's original jurisdiction.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiffs' claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

PARTIES

4. Plaintiff Leo Thorbecke is a resident and citizen of Indiana.

5. Plaintiff Marjorita Dean is a resident and citizen of Ohio.

6. Defendant MCG Health, LLC is a Washington limited liability company with its principal place of business in Seattle, Washington.

7. Defendant MCG Health is a division of Hearst Corporation, a Delaware corporation.

FACTUAL ALLEGATIONS

I. MCG Health

8. Defendant MCG Health is a Seattle-based software company that "provides patient care guidelines to health care providers and health plans."[1]

9. A majority of U.S. health plans and nearly 2,600 hospitals utilize Defendant's software and are Defendant's customers.

[1] https://www.businesswire.com/news/home/20220610005006/en/Notice-Provided-to-Individuals-Regarding-MCG-Data-Security-Incident

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

10. Patients and members of Defendant's customers, like Plaintiffs and Class members, provided certain Personal Identifying Information ("PII") and Protected Health Information ("PHI") to their healthcare providers which is required as a condition of medical treatment. Plaintiffs' and Class members' PII and PHI was then provided to Defendant.

The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.[2]

11. As a large technology company with an acute interest in maintaining the confidentiality of the PII and PHI entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII and PHI in its possession.

12. Defendant represents to patients and members and the public that it possesses robust security features to protect PII and PHI.

II. The Data Breach

13. On June 10, 2022, Defendant announced in a press release that it was investigating a data security incident that it had initially discovered on March 25, 2022. Defendant's investigation included assistance of a forensic investigation firm.[3]

14. The investigation determined that "an unauthorized party previously obtained personal information about some patients and members of certain MCG customers. The affected patient or member data included some or all of the following data elements: names, Social

[2] *Id.*
[3] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender."[4]

15. On or about April 22, 2022, MCG notified its affected customers (i.e., healthcare systems) of the breach. In turn, MCG customers began notifying their patients in June 2022.

16. Defendant sent a letter to Plaintiffs Dean and Thorbecke dated June 10, 2022, notifying them of the breach. *See* Exhibit A and Exhibit B.[5]

17. Defendant's letter also offered two years of free identity protection services to affected patients and members.

18. Defendant did not state why it was unable to detect the unauthorized individuals accessing Defendant's servers.

19. Defendant did not state why it waited for nearly three months before notifying affected patients and members.

20. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

III. Injuries to Plaintiffs and the Class

21. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs' PII and PHI, Plaintiffs and the Class have been damaged.

22. Plaintiffs and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages,

[4] *Id.*
[5] *See also* https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

23. In addition to the irreparable damage that may result from the theft of PII and PHI, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

24. In addition to fraudulent charges and damage to their credit, Plaintiffs and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

25. Additionally, Plaintiffs and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII and PHI is used, the diminution in the value and/or use of their PII and PHI entrusted to Defendant, and loss of privacy.

[6] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

IV. The Value of Personal Identifying Information

26. It is well known that PII and PHI, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

27. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[7]

28. People place a high value not only on their PII and PHI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[8]

29. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[9] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[10]

---

[7] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[8] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[9] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[10] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

30. The PII and PHI of minors (like the dependents of many Class Members) can be used to receive illicit gains through methods such as credit card fraud with newly created accounts. The fact that a minor's social security number has not yet been used for financial purposes actually makes it more valued by hackers rather than less. The "blank slate" credit file of a child is much less limited than the potentially low credit score of an adult. Social security numbers that have never been used for financial purposes are uniquely valuable as thieves can pair them with any name and birthdate. After that happens, thieves can open illicit credit cards or even sign up for government benefits.[11]

V. Industry Standards for Data Security

31. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, and Equifax, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII and PHI, as well as of the foreseeable consequences of its systems being breached.

32. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

[11] Richard Power, "Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers," Carnegie Mellon CyLab, https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII and PHI;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

33. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[12] and protection of PII and PHI[13] which includes basic security standards applicable to all types of businesses.

34. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

---

[12] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[13] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

35. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[14]

36. Because Defendant was entrusted with patients and members' PII and PHI, it had, and has, a duty to patients and members to keep their PII and PHI secure.

37. Patients and members, such as Plaintiffs and the Class, reasonably expect that when they provide PII and PHI to Defendant, it will safeguard their PII and PHI.

38. Nonetheless, Defendant failed to prevent the data breach discussed below. Had Defendant properly maintained and adequately protected its systems, it could have prevented the data breach.

CLASS ALLEGATIONS

39. Plaintiffs, individually and on behalf of all others, bring this class action pursuant to Fed. R. Civ. P. 23.

40. The proposed Class is defined as follows:

Nationwide Class: All persons whose PII and PHI was maintained on Defendant MCG Health, LLC's servers that were compromised in the Data Breach.

41. Plaintiffs reserve the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

42. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiffs, Defendant has

[14] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

reported that the number of patients and members affected by the data breach is as high as 1.1 million.[15] The Class Members can be readily identified through Defendant's records.

43. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII and PHI;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and the Class's PII and PHI secure and prevent loss or misuse of that PII and PHI;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiffs' and Class's PII and PHI;

h. Whether Defendant's conduct was intentional, willful, or negligent;

[15] https://www.hipaajournal.com/data-theft-incidents-reported-at-choice-health-mcg-health-goodman-campbell-brain-and-spine/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

44. *Typicality*: The claims or defenses of Plaintiffs are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiffs, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiffs.

45. *Adequacy*: Plaintiffs will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiffs have retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

46. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiffs and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

47. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

48. *Manageability*: Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

49. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

50. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

51. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

//

//

//

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Class)

52. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

53. Defendant owed a duty of care to Plaintiffs and Class members to use reasonable means to secure and safeguard the entrusted PII and PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and Class members would be harmed by such exposure of their PII and PHI.

54. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and Class members, on the other hand. The special relationship arose because Plaintiffs and Class members entrusted Defendant with their PII and PHI, Defendant accepted and held the PII and PHI, and Defendant represented that the PII and PHI would be kept secure pursuant to its data security policies. Defendant alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the data breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

55. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and PHI. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

56. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

57. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII and PHI provided to it by Plaintiffs and Class members, thus resulting in unauthorized third-party access to the Plaintiffs' and Class members' PII and PHI.

58. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs' and Class members' PII and PHI within its possession, custody, and control.

59. As a direct and proximate cause of failing to use appropriate security practices, Plaintiffs' and Class members' PII and PHI was disseminated and made available to unauthorized third parties.

60. Defendant admitted that Plaintiffs' and Class members' PII and PHI was wrongfully disclosed as a result of the breach.

61. The breach caused direct and substantial damages to Plaintiffs and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and PHI and the greatly enhanced risk of credit fraud or identity theft.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

62. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII and PHI; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class members' PII and PHI.

63. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their PII and PHI would not have been compromised.

64. Neither Plaintiffs nor the Class contributed to the breach or subsequent misuse of their PII and PHI as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiffs and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiffs and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII and PHI, including the amount of time Plaintiffs and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiffs and the Class to the extent their PII and PHI has been diminished in value because Plaintiffs and the Class no longer control their PII and PHI and to whom it is disseminated.

//

//

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

COUNT II
INVASION OF PRIVACY
(on behalf of the Class)

65. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

66. Defendant invaded Plaintiffs' and the Class's right to privacy by allowing the unauthorized access to their PII and PHI and by negligently maintaining the confidentiality of Plaintiffs' and the Class's PII and PHI, as set forth above.

67. The intrusion was offensive and objectionable to Plaintiffs, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and the Class's PII and PHI was disclosed without prior written authorization from Plaintiffs and the Class.

68. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class provided and disclosed their PII and PHI to Defendant privately with an intention that the PII and PHI would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

69. As a direct and proximate result of Defendant's above acts, Plaintiffs' and the Class's PII and PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class suffered damages as described herein.

70. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class's PII and PHI with a willful and conscious disregard of their right to privacy.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

71. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs and the Class great and irreparable injury in that the PII and PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Defendant may freely treat Plaintiffs' and the Class's PII and PHI with sub-standard and insufficient protections.

COUNT III
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT
(RCW 19.86.010 *et seq.*)
(on behalf of the Class)

72. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

73. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

74. Defendant is a "person" as described in RWC 19.86.010(1).

75. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

76. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

77. In the course of conducting their business, Defendant committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

78. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealing from Plaintiffs and Class Members the unauthorized release and disclosure of their Private Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information, medical information, and identities.

79. Defendant's above-described "unfair or deceptive acts or practices" in violation effects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

80. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

81. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiffs and Class Members' business and property. Plaintiffs and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her Private Information; (5) deprivation of the value of his or her Private Information, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them

82. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

83. Plaintiff, on behalf of Plaintiffs and the Class Members, also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of Plaintiffs and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

//

//

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

COUNT IV
BAILMENT
(on behalf of the Class)

84. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

85. Plaintiffs and the Class provided, or authorized disclosure of, their PII and PHI to Defendant.

86. In allowing their PII and PHI to be made available to Defendant, Plaintiffs and the Class intended and understood that Defendant would adequately safeguard their PII and PHI.

87. For its own benefit, Defendant accepted possession of Plaintiffs' and the Class's PII and PHI.

88. By accepting possession of Plaintiffs' and the Class's PII and PHI, Defendant understood that Plaintiffs and the Class expected Defendant to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their personal information.

89. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and the Class's personal information, resulting in the unlawful and unauthorized access to and misuse of their PII and PHI.

90. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

91. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiffs and the Class entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT V
BREACH OF IMPLIED CONTRACT
(on behalf of the Class)

92. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

93. Defendant invited Plaintiffs and the Class to provide their PII and PHI to Defendant. As consideration for the benefits Defendant was to administer, Plaintiffs and the Class provided their PII and PHI to Defendant. When Plaintiffs and the Class provided their PII and PHI to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII and PHI and only use it solely to administer benefits. As part of the offer, Defendant would safeguard the PII and PHI using reasonable or industry-standard means.

94. Accordingly, Plaintiffs and the Class accepted Defendant's offer to administer benefits and provided Defendant their PII and PHI.

95. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiffs' and the Class's PII and PHI.

96. The losses and damages Plaintiffs and the Class sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiffs and the Class continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

remedy for the breaches alleged herein, Plaintiffs and the Class are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII and PHI from unlawful exposure.

97. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and it is liable to Plaintiffs and the Class for associated damages and specific performance.

COUNT VI
BREACH OF CONFIDENCE
(on behalf of the Class)

98. Plaintiffs hereby incorporate by reference all preceding paragraphs as though fully set forth herein.

99. As alleged above, Plaintiffs and the Class had agreements with Defendant, both express and implied, that required Defendant to keep their PII and PHI confidential.

100. Defendant breached that confidence by disclosing Plaintiffs' and the Class's PII and PHI without their authorization and for unnecessary purposes.

101. As a result of the data breach, Plaintiffs and the Class suffered damages that were attributable to Defendant's failure to maintain confidence in their PII and PHI.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiffs as Representatives of the proposed Class, and appointing the law firms representing Plaintiffs as counsel for the Class;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand trial by jury.

Dated: June 21, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
s/ Rebecca L. Solomon
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
rsolomon@tousley.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com

Charles E. Schaffer*
Nicholas Elia*
LEVIN, SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Counsel for Plaintiffs and Putative Class Members

** Indicates Pro Hac Vice application forthcoming*

Exhibit A

MCG Health, LLC
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 10, 2022

[redacted]

[redacted]DEAN MARJORITA
[redacted]

Dear Dean Marjorita:

MCG Health, LLC ("MCG") provides patient care guidelines to health care providers and health plans, including [redacted]. We are writing on behalf of [redacted] to notify you of a recent data security issue at MCG that affects certain of your personal information.

MCG determined on March 25, 2022 that an unauthorized party previously obtained certain of your personal information that matched data stored on MCG's systems. The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

Upon learning of this issue, we took steps to understand its nature and scope. A leading forensic investigation firm was retained to assist in the investigation. Additionally, we are coordinating with the FBI. We have deployed additional monitoring tools and will continue to enhance the security of our systems.

We regret any concern this issue may cause. We are alerting you about this issue so you can take steps to help protect your information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

In addition, we have arranged to offer you identity protection and credit monitoring services for two years at no cost to you. The attached Reference Guide provides information on activation and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have questions regarding this issue, please call 1-866-475-7221 Monday – Friday, 6 am to 8 pm PT; Saturday – Sunday, 8 am to 5 pm PT.

Sincerely,

Jon Shreve

Jon Shreve
President and CEO

[redacted]

Exhibit B

MCG Health, LLC
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 10, 2022

[redacted]
LEO THORBECKE
[redacted]

Dear Leo Thorbecke:

MCG Health, LLC ("MCG") provides patient care guidelines to health care providers and health plans, including [redacted]. We are writing on behalf of [redacted] to notify you of a recent data security issue at MCG that affects certain of your personal information.

MCG determined on March 25, 2022 that an unauthorized party previously obtained certain of your personal information that matched data stored on MCG's systems. The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

Upon learning of this issue, we took steps to understand its nature and scope. A leading forensic investigation firm was retained to assist in the investigation. Additionally, we are coordinating with the FBI. We have deployed additional monitoring tools and will continue to enhance the security of our systems.

We regret any concern this issue may cause. We are alerting you about this issue so you can take steps to help protect your information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

In addition, we have arranged to offer you identity protection and credit monitoring services for two years at no cost to you. The attached Reference Guide provides information on activation and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have questions regarding this issue, please call 1-866-675-7221 Monday – Friday, 6 am to 8 pm PT; Saturday – Sunday, 8 am to 5 pm PT.

Sincerely,

Jon Shreve

Jon Shreve
President and CEO [redacted]

H9734-L01